WHAT IS CLAIMED IS:

1. A method for communicating a document from a sender to a recipient, wherein the recipient is enabled to verify the contents of the document, comprising the steps of:

defining a format for document transmission in a document representation language suitable for processing documents including both text and operable code, said format including either (a) an algorithm for encoding the document according to a private key known only to the sender, or (b) a link to a site providing an algorithm for so processing the document;

at a transmitting location:

employing said format to generate an encoded message, said message including a version of said document that is encoded according to the sender's private key, includes an identification of the sender, and also includes one of (a) an algorithm for decoding the document according to a private key known only to the sender, or (b) a link to a site providing an algorithm for so decoding the document; and

transmitting said document; and

at a receiving location:

receiving the encoded message;

employing the identity of the sender to obtain a public key corresponding to said private key and said decoding algorithm; and

employing said public key and the decoding algorithm to decode the document to verify its contents.

2. The method of claim 1, wherein said template includes definition of fields for user insertion of specific information, and said encoded message includes definition of said fields and information placed therein by a user.

3. The method of claim 1, wherein said encoding and decoding algorithms collectively perform the following steps:

collecting the elements of the host document into a data structure that represents the canonical form of the document at the time of signature;

reducing the canonical data structure into a bit sequence suitable for processing by an electronic signature algorithm;

obtaining a cryptographic key;

passing the bit sequence and key material to an electronic signature algorithm, which then provides a suitably encoded message;

retrieving the output of the signature algorithm;

notifying human users of the results of signature verification processes; and

passing the signature and signed data to host applications.

4. A method for employing self-signing document objects (SSDOs) for communication of messages capable of verification by a recipient, comprising the steps of:

defining a Template SSDO (T-SSDO) containing an embedded electronic signature processing and verification program, and which is capable of accepting application-specific additional elements;

adding application-specific elements to the T-SSDO, to create a Fabricated SSDO (F-SSDO;

making the F-SSDO available to a user, such that the user can retrieve and interact with the F-SSDO, resulting in a Processed SSDO (P-SSDO);

permitting the user to electronically sign the P-SSDO, causing execution of the embedded signature processing program, in response to which the signature processing program: (1) collects and encodes the elements of the P-SSDO

into a data structure including the elements of the P-SSDO in a predefined sequence, (2) decomposes the data structure representing the P-SSDO into a linear sequence of bits, (3) retrieves the user's private signature key, and (4) generates and returns an electronic signature, referred to as an S-SSDO, responsive to said linear series of bits, said private key, and a prdetermined algorithm;

storing the S-SSDO for subsequent verification;

transmitting the S-SSDO to the intended recipient; and

executing the signature verification program embedded in the S-SSDO, by: (1) recreating the data structure, (2) decomposing the data structure to generate a bit sequence, (3) retrieving the signer's public key information; and (4) employing the bit sequence, signature data, and signer's public key material to verify the origin and structural integrity of the P-SSDO.

5. A method for communicating an encrypted message from a sender to a recipient, comprising the steps of:

employing a secret key unique to the sender to encrypt the message, using a known encryption algorithm having a corresponding known decryption algorithm;

transmitting the encoded message to the recipient in a language permitting executable software instructions to be embedded in a message also including data, and employing a message format including the decryption algorithm, or a link to a site providing the decryption algorithm, as executable instructions, and the encoded message as data;

separately transmitting the secret key to the recipient; and

employing the decryption algorithm embedded in the message or the link to a site providing the algorithm and the secret key to decrypt the message.

6. The method of claim 5, wherein said message format is defined by provision of a template wherein the algorithm is

provided as part of a cipher management program, said template accepting application-specific elements such as the message to be transmitted.

7. The method of claim 6, wherein said cipher management program performs the fllowing functions:

Collects the elements of the message to be communicated into a data structure that represents the canonical form of the document;

Reduces the canonical data structure into a bit sequence suitable for processing by a cryptographic algorithm;

Obtains the secret key;

Passes the bit sequence and key material to a cryptographic algorithm;

Retrieves the output of the cryptographic algorithm;

Notifies a user of the results of encryption/decryption processes; and

Passes the plaintext or ciphertext data to host applications.

8. A method for employing self-encrypting document objects (SEDOs) for communication of encrypted messages capable of decryption by a recipient, comprising the steps of:

defining a Template SEDO (T-SEDO) containing an embedded cipher management program, and which is capable of accepting application-specific additional elements;

adding application-specific elements to the T-SEDO, to create a Fabricated SSDO (F-SEDO;

making the F-SEDO available to a user, such that the user can retrieve and interact with the F-SEDO, resulting in a Processed SEDO (P-SEDO);

permitting the user to indicate a desire to encrypt the P-SEDO, causing execution of the embedded cipher management program, in response to which the cipher management program: (1) collects and encodes the elements of the P-SEDO into a

data structure including the elements of the P-SEDO in a predefined sequence, (2) decomposes the data structure representing the P-SEDO into a linear sequence of bits, (3) retrieves the user's secret encryption key, and (4) generates and returns an encrypted form of the P-SEDO, referred to as an E-SEDO, responsive to said linear series of bits, said secret encryption key, and a prdetermined algorithm;

storing the E-SEDO for subsequent verification;

transmitting the E-SSDO to the intended recipient; and

executing the decryption program embedded in the E-SEDO, by: (1) recreating the data structure, (2) decomposing the data structure to generate a bit sequence, (3) retrieving the signer's secret encryption key information; and (4) employing the bit sequence and signer's secret encryption key material to decrypt the E-SEDO.